

## AMENDMENT TO THE SPECIFICATION

Please amend the paragraph starting on page 9, line 17 as follows:

"In the encryption stage ~~40~~<sup>50</sup>, Alice generates an encryption ephemeral private key as random integer value  $x$  and computes a corresponding encryption ephemeral public key  $X$ , where  $X = xG$ . As described above, the set  $(X, x)$  represents the ephemeral key pair produced in the encryption scheme. With this information, Alice uses Bob's public key  $B$  to compute secret key  $K$  ~~20~~, given by  $K = xB$ . Alice then encrypts the message producing  $ciphertext = encrypt(K, message)$  ~~22~~."